Approved for use through 07/31/20.. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL for FY 2005

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	($) 500

Complete If Known	
Application Number	09/726,766
Filing Date	November 29, 2000
First Named Inventor	John M. Davidson
Examiner Name	Phillip C. Lee
Art Unit	2154
Attorney Docket No.	020533.0340 (2001P21477US)

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify) : _____

☒ Deposit Account Deposit Account Number: 19-2179 Deposit Account Name: Siemens Corporation

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☒ Charge any additional fee(s) or underpayments of fee(s) Under 37 CFR 1.16 and 1.17 ☒ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	Fee ($)	Fee($)	Fee($)	Fee($)	Fee($)	Fee($)	Fees Paid ($)
Utility	300	150	500	250	200	100	____
Design	200	100	100	50	130	65	____
Plant	200	100	300	150	160	80	____
Reissue	300	150	500	250	600	300	____
Provisional	200	100	0	0	0	0	____

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee($)	Fee Paid ($)
____ -20 or HP=	____	x ____	= ____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee($)	Fee Paid ($)
____ - 3 or HP=	____	x ____	= ____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims	
Fee ($)	Fee Paid ($)
____	____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
____ - 100 =	____	/ 50 = ____ (round up to a whole number) x		= ____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	____
Other (e.g., late filing surcharge) : **Filing a Brief in support of an appeal 1402/2402**	**500**

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 34,733	Telephone 407-736-2415
Name (Print/Type)	DANIEL J. STAUDT		Date May 19, 2006

RECEIVED
CENTRAL FAX CENTER

MAY 19 2006

SIEMENS

PATENT
Attorney Docket No. 2001P21477US (020533.340)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Inventor:	John M. Davidson et al.	)	Group Art Unit: 2154
Serial No.:	09/726,766	)	Examiner: Philip C Lee
Filed:	November 29, 2000	)	

Title: METHOD AND APPARATUS FOR TUNNELED COMMUNICATION IN AN ENTERPRISE NETWORK

Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

APPELLANTS BRIEF

This Appeal Brief relates to an appeal from the final rejection of claims 1, 3-24, 26-33 and 35-45 in the Office Action mailed September 21, 2005.

05/22/2006 STEUMEL1 00000033 192179 09726766
01 FC:1402 500.00 DA

Real Party in Interest

This application is assigned to Efficient Networks, Inc. of Dallas, Texas (currently know as Siemens Subscriber Networks, LLC). Efficient Networks is a wholly owned subsidiary of Siemens Corporation of Iselin, New Jersey.

Related Appeals and Interferences

There are no prior and pending appeals, interferences or judicial proceedings known to Applicants, Applicants' legal representative, or Assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

Status of Claims

Claims 1, 3-24, 26-33 and 35-45 stand rejected by the Office Action mailed December 21, 2005 and are presently under appeal in this proceeding. No other claims stand rejected, allowed, withdrawn, objected to, or canceled.

Status of Amendments

No amendment has been filed subsequent to the final rejection.

Summary of Claimed Subject Matter

Independent Claim 1

Referring to Figures 1 and 2, independent claim 1 recites a method of communicating with an element within an enterprise network 12, comprising:

at a first client 16, 17, encapsulating a first point-to-point protocol signal 124 within a network address request header 114, the first point-to-point protocol signal 124 comprising a point-to-point protocol header 118 that includes an identifier of a second client (see e.g., para. 5); and

communicating the encapsulated signal 100 toward a tunneling server 32 (see e.g., para. 5).

Dependent Claim 5

Referring to Figure 2, dependent claim 5 recites the method of claim 1, wherein the first point-to-point protocol signal 124 further comprises a payload 120 including information to be applied to an application residing at the second client (see e.g., para. 10, 87).

Dependent Claim 7

Referring to Figure 2, dependent claim 6 recites the method of claim 1, wherein the first point-to-point protocol signal 124 further comprises a payload 120 including at least a portion of an application to be installed on the second client (see e.g., para. 10, 87).

Independent Claim 12

Referring to Figures 1 and 2, independent claim 12 recites a computer readable medium operable to execute the following steps on a processor of a computer:

at a first client 16, 17, encapsulating a first point-to-point protocol signal 124 within a network address request header 114, the first point-to-point protocol signal 124 comprising a point-to-point protocol header 118 that includes an identifier of a second client (see e.g., para. 6); and

communicating the network address request encapsulated signal 100 toward a tunneling server 32 (see e.g., para. 6).

Dependent Claim 15

Referring to Figure 2, dependent claim 15 recites the computer readable medium of claim 12, wherein the first point-to-point protocol signal 124 further comprises a payload 120 including information to be applied to an application residing at the second client (see e.g., para. 10, 0087).

Dependent Claim 16

Referring to Figure 2, dependent claim 16 recites the computer readable medium of claim 12, wherein the first point-to-point protocol signal 124 further comprises a payload 120 including at least a portion of an application to be installed on the second client (see e.g., para. 10, 87).

Independent Claim 19

Referring to Figures 1, 2 and 3, independent claim 19 recites a method of tunneling in an enterprise network comprising a plurality of clients coupled 16 to a tunneling server 18 by at least one router 18, the method comprising:

at a first client 16, generating point-to-point protocol signal 124 (see e.g., para. 7);

encapsulating the point-to-point protocol signal 124 within a network address request header 214 (see e.g., para. 7);

communicating the encapsulated signal 200 toward a tunneling server operable 32 to identify and remove the network address request header 214, to encapsulate the point-to-point protocol signal 124 within a network address response header 214, and to communicate the encapsulated response signal 300 toward a second client 16, 17 (see e.g., para. 7).

Independent Claim 24

Referring to Figures 1, 2, 3 and 4, independent claim 24 recites in an enterprise network comprising at least one client coupled to a tunneling server by a router having a routing table indexed by data channel addresses, a first client comprising:

a protocol stack 40, 52 operable to generate a first point-to-point protocol signal 124 comprising a point-to-point protocol header 118 that includes an identifier of a second client 16, 17 (see e.g., para. 8); and

a tunneling module 50 operable to encapsulate the first point-to-point encapsulated signal 124 within a network address request header 114, 214 comprising a Dynamic Host Configuration Protocol DISCOVER header or a Bootstrap Protocol REQUEST header(see e.g., para. 8);

wherein the first client 16, 17 is operable to communicate the encapsulated signal 100 toward the router 18 for forwarding to the tunneling server 32 without reference to the routing table (see e.g., para. 8).

Independent Claim 33

Referring to Figures 1, 2 and 4, independent claim 33 recites in an enterprise network, a client having an enterprise protocol stack operable to process signals received from a data channel and associated with a data channel address, the client comprising:

a tunneling module 50 operable to receive a first point-to-point protocol signal 124 encapsulated within a network address response header 114, 314 and to remove the network address response header 114 to expose the first point-to-point protocol signal 124, the first point-to-point protocol signal comprising a point-to-point protocol header 118 that includes an identifier of a client, the network address response header(see e.g., para. 9); and

a private protocol stack 52 operable to receive the first point-to-point protocol signal 124 from the tunneling module and to communicate at least a portion of a payload 120 of the first point-to-point protocol signal to a socket layer 54 coupled to an application 56 residing at the client(see e.g., para. 9).

Grounds for Rejection to be Reviewed

Whether claims 12-16 and 42 are unpatentable under U.S.C. § 101 as containing non-statutory subject matter.

Whether claims 1, 3, 12-13, 19-20, 24, 33, and 37 are unpatentable under U.S.C. § 103 as being anticipated over May (US Patent App. 2001/0030977) in view of Shukla (US Patent App. 2002/0042875) and Araujo et al. (USPN 6,301, 229).

Whether claims 4, 10-11, 14, 18, 21, 23, 28-29, 31-32, 38 and 41-45 are unpatentable under U.S.C. § 103 as being anticipated over May, Shukla, Araujo in view of Inoue et a. (US Patent App. 2002/000741).

Whether claims 5-7, 15-16, 30 and 35-36 are unpatentable under U.S.C. § 103 as being anticipated over May, Shukla, Araujo in view of Singhal et al. (USPN 6,633,761)

Whether claims 8, 17, 22, 26 and 39 are unpatentable under U.S.C. § 103 as being anticipated over May, Shukla, Araujo in view of Zhang (USPN 6,108,345)

Particularly, if:

a) May teaches or suggests encapsulating a first point-to-point signal within a network address header,

b) Shukla teaches or suggests encapsulating a first point-to-point signal within a network address header,

c) Araujo teaches or suggests a tunneling server operable to identify the network address request header, to remove the network address request header, or to encapsulate the point-to-point protocol signal within a network address response header, or

d) Singhal teaches or suggests the first point-to-point protocol signal comprising a payload inforamtion information that is applied to an application at the second client or the payload including at least a portion of an application to be installed on the second client.

Appellants' Argument

A. Applicants' Invention

A network element is a communication or computing device, such as a computer or personal digital assistant. Network elements can communicate message signals with each other via a communication system including routers and tunneling protocols. Routers use a data channel address of the signal's destination address to forward the message. Tunneling protocols provide secure connections between network elements implementing the tunneling protocols. However, several limitations exist regarding with routing and tunneling in these systems.

One such limitation occurs when a network element is connected to the system behind a firewall. A firewall limits access between the network elements by filtering out messages or packets toward the connected network element. This is problematic when the firewall filters out tunneling protocols because filtering out the tunneling protocols prevents the network elements from participating in tunneling. Past solutions to this firewall problem include using a Hypertext Transfer Protocol (HTTP) header to fool the firewall into accepting the packet since it appears to be an HTTP signal.

Another limitation is that network elements without data channel addresses are ineligible to participate in tunneling using conventional tunneling protocols. As previously discussed, a router uses a data channel address to forward the message. The data channel address is a network address for example Internet Protocol (IP) address, which is used to index a route table to obtain information on forwarding the message. The HTTP solution does not solve the limitation of the network elements without data channel address being ineligible to participate in tunneling.

One aspect of Applicants' present invention involves at a first client encapsulating a point-to-point signal within a network address request header, the point-to-point signal comprising a header having an identifier of a second client, and communicating the encapsulated signal toward a tunneling server. The network address request header comprises a message to request a network address. For example, the network address request header comprises a Dynamic Host Configuration Protocol (DHCP) Discover, Bootstrap protocol, or any other message to request a network address. The identifier of the second client identifies the destination client for which the encapsulated packet is intended. This aspect of the invention

advantageously allows the first client to communicate a point-to-point signal to a tunneling server even if the tunneling server is behind a firewall since the firewall will interpret the signal as a network address request signal.

Another aspect of the present invention involves encapsulating the first point-to-point protocol signal within a tunneling header prior to encapsulating the first point-to-point protocol signal within the network address request header, the tunneling header operable to facilitate a tunneling session between the first client and the tunneling server. This aspect of the present invention facilitates a tunneling session between the first client and the tunneling server which may be used in future communication.

Another aspect of the present invention involves the identifier comprising a control channel address of the second client, the control channel address being different from any data channel address recognized by the router. As previously discussed, data channel address is a network address used to index the routing table. This advantageously allows the second client to participate in tunneling when it does not have a data channel address.

Another aspect of the present invention involves the tunneling server operable to identify and remove the network address request header, to encapsulate the point-to-point protocol signal within a network address response header, and to communicate the encapsulated response signal toward a second client. In this aspect of the invention the tunneling server relays signals between the first and second client by first recognizing the received signal as one to be relayed. Then the tunneling server removes the network address request header from the point-to-point protocol signal. Next the point-to-point protocol signal is encapsulated in a network address response header and then communicated toward the second client. Thus, by this aspect of the invention, the first and second client may communicate with each other via the tunneling server even if one or both clients are behind a firewall or event if one or both clients do not have a data channel address.

Another aspect of the present invention involves the point-to-point protocol signal including a payload. The payload, for example, having information to be applied at an application at the second client or having a portion of an application to be installed on the second client.

B. The Cited Art

a.) May

May teaches a proxy method for dynamically assigning an Internet Protocol (IP) address to a computer configured for operation on a wide area network (WAN) using a local area network (LAN) address assignment format (Abstract). In May, the computer sends a PPP over Ethernet (PPPoE) packet to a modem wherein the modem is a proxy for the computer to request the IP address (see e.g., para. 49 and also Fig. 5). Then, a translator in the modem converts the packets from the PPP format into a DHCP format (see e.g., para 49). Next, the modem sends the DHCP request toward a DHCP server (see e.g., para. 53) and the DHCP server sends a response having the IP address (see e.g., para. 54). Then, the modem sends the IP address to the computer in a PPPoE packet (see e.g., para. 54). Thus, by May's method, a computer can obtain a dynamic IP address via DHCP when the computer is in an environment otherwise not capable of dynamically obtaining an IP address.

c.) Shukla

Shukla teaches how to achieve an end-to-end secure communication over LANs, virtual private networks (VPNs), and in network-to-network connections, wherein compatibility with network address translation (NAT), Internet Control Message Protocol (ICMP), and many quality of service (QoS) protocols is also achieved. (see e.g., para. 40). In Shukla, information in packets is encrypted to provide the secure communication, wherein data packets are encrypted differently than control packets (see e.g., para 41).

b.) Araujo

Araujo teaches improving network performance in a communication system by distributing certain recurring protocol processing functions to a customer premises equipment (CPE) (see e.g., col. 3 lines 11-15). In Araujos' communication system, an end station, such as a CPE, communicates with another end station, such as a remote access server (RAS), via the network. The CPE for example may be a computer. The network, according to Araujo, includes

one or more intermediate devices to facilitate the communication, wherein the end station is connected to an intermediate device via a link (see e.g., col 3 lines 48-51).

Araujo teaches establishing according to a PPP a session between the CPE and the RAS via the intermediate device(s). In order to take data from several CPEs and multiplex the data on a single virtual circuit (VC) and to separate the aggregated data from the VC to the separate CPEs, Araujo teaches using a multiplexing scheme, such as, a Layer 2 Tunneling Protocol (L2TP) to establish a L2TP tunnel between the intermediate device and the RAS.

d.) Sighal

Singhal provides a seamless mobility in a short-range wireless networking environment for a mobile device. Singhal includes client devices, handoff management points (HMP), handoff core server(s); and application servers as the major components in the environment (see e.g. col. 3 lines 52-56). Singhals' core server provides services to the HMPs as users roam through the environment (see e.g., col 4 lines 17-21) and maintains information about HMPs that have registered with the core server (see e.g., col 4 lines 25-28, Figures 2, 4, 5). In addition, the core server maintains information about devices communicating via an HMP (see e.g., col 4 lines 25-28, Figure 3).

Singhal teaches that a client can perform a standard DHCP request that will always be handled by the core server and results in the assignment of the same IP address for a device, regardless of which HMP receives the request (see e.g., col. 10, lines 8-13). Thus a device can advantageously have the same IP address as the device roams though the system.

Singhal further teaches that a core management sever may be coupled to a plurality of core servers (see e.g., col 14, lines 1-3). The core management server provides services on behalf of the core servers, including monitoring, remote diagnostics, configuration services and other management services (see e.g., col 14, lines 1-12). In order to provide these services the core servers include APIs, which are exposed to the core management server (see e.g., col. 14, lines 26-27).

e.) Inoue

Inoue teaches a packet relay device at a first sub-network for processing a request message for a radio terminal (see e.g., abstract). The first sub-network is connected to the

terminal by a downlink communication interface via a first radio base station (see e.g., abstract, Figure 2). The downlink communication interface allows communication to the terminal so that the terminal only receives data via the downlink communication interface (see e.g., abstract). A second sub network is connected to the terminal via a bi-direction communication interface via a second radio base station (see e.g., abstract, Figure 2). The bi-direction communication interface allows communications to and from the terminal. The first sub-network and the second sub-network are connected via a backbone network (see e.g., para.2), such as the Internet (see e.g., para. 47).

Inoue teaches that a request message, such as DHCP, is encapsulated within an IP packet and transferred from the terminal to the packet relay device through the second sub-network (see e.g., para 82), and a response to the request message is transferred from the packet relay device to the radio terminal. (see e.g., abstract). Thus by Inoues' method a first sub-network that otherwise could not access the backbone can have access the backbone via the second sub-network.

e.) Zhang

Zhang teaches an improved device for connecting networks (see e.g., col 2 lines 33-34) wherein a tunneling protocol data package includes a MAC identifier.

Applicants agree with the Examiner's reading of Zhang.

C. Section 101 Rejections of Claims 12-18 and 42

In the Advisory Action mailed December 21, 2005, the Examiner states that claims 12-18 and 42 are unpatentable under 35 U.S.C. § 101 as containing non-statutory subject matter.

The Examiner states that a computer readable medium that includes carrier wave (electro-magnetic signal) is non-statutory subject matter. Pursuant to the "Interim Guidelines for Examination of Patent Applications for Subject Matter Eligibility", the Examiner apparently reads Applicants' signal as a carrier wave. However, Applicants claims do not use the term "signal" as a carrier wave, rather, the term signal is used to refer data in a message format (see e.g. Figures 2 and 3, Office Action Response mailed April 8, 2005). Therefore, the rejections of the "Interim Guidelines for Examination of Patent Applications for Subject Matter Eligibility"

are inapplicable. Notwithstanding, Applicants would be willing to amend the term "signal" to "message data" or other suitable term in order to overcome the Section 101 rejections.

D. Section 103 Rejections of Independent Claims 1, 12, and 24

In the Office Action mailed September 21, 2005, the Examiner states that independent claims 1, 12, and 24 are unpatentable under 35 U.S.C. § 103 as obvious over May in view of Shukla and in further view of Araujo (para. 7, 9-13, 19-23).

The Examiner asserts that "May teaches converting a first point-to-point protocol signal into a network address request header (para. 49)." Applicants' claim however recites encapsulating a first point-to-point protocol signal within a network address header. Encapsulating is completely different than conversion. Encapsulation appends information onto the packet to encapsulate the packet whereas conversion changes the packet from one format to another format.

The Examiner further asserts that Shukla teaches that packet conversion between protocol layers comprises each protocol layer encapsulating its own header before transmitting to the next layer (para. 3, Figure 5). However, Applicants claim recites encapsulating a first point-to-point protocol signal within a network address request header and not encapsulating a network header within itself or encapsulated a first point-to-point protocol signal within itself. Applicants respectfully note that according to the Examiners citation, paragraph 3 and the Open System Interconnect (OSI) stack disclose that a header is encapsulating the data before transmitting to the next layer and not that a header is encapsulating is own header.

In view of the above, it is respectfully submitted that independent claims 1, 12, and 24 are patentable.

E. Section 103 Rejection of Independent Claim 19

In the Office Action mailed September 21, 2005, the Examiner states that independent claim 19 is unpatentable under 35 U.S.C. § 103 as obvious over May in view of Shukla and in further view of Araujo (para. 7, 14-18).

The Examiner asserts that Araujo teaches communicating the encapsulated signal toward a tunneling server operable to identify the protocol header (col. 13, lines 37-47). However, Applicants' claim recites communicating the encapsulated signal (a first point-to-point protocol signal encapsulated within a network address request header) toward a tunneling server operable to identify the network address request header. Applicants respectfully submit that Araujo teaches identifying a tunneling header control frame (see e.g., col. 13, lines 44-46) or data frame (see e.g., col. 13, 48-50), which is used for a tunneling protocol. Applicants' network address request header is used to request a network address wherein a tunneling header is used to supply tunneling information. A tunneling header is completely different than a network address request header.

The Examiner further asserts that Araujo teaches the tunneling server operable to remove the protocol header (col. 13, lines 37-47), to encapsulate the point-to-point protocol signal within a protocol response header and to communicate the encapsulated response signal toward a second client (col. 13, lines 34-36, 48-56). However, Applicants' claim recites a tunneling server operable to remove the network address request header, to encapsulate the point-to-point protocol signal within a network address response header, and to communicate the encapsulated response signal toward a second client. As previously discussed, Applicants' network address request header is not a tunneling header. Furthermore, Applicants respectfully submit that Araujo teaches the tunneling server operable to forward the request signal without removing the tunneling header toward a second client and that the second client will remove the header. Moreover, Applicants respectfully submit that Araujo does not teach that the server operable to encapsulate the point-to-point signal let alone encapsulate the signal in a network address response header or even a response header.

In view of the above, it is respectfully submitted that independent claim 19 is patentable.

F. Section 103 Rejection of Independent Claim 33

In the Office Action mailed September 21, 2005, the Examiner states that independent claim 33 is unpatentable under 35 U.S.C. § 103 as obvious over May in view of Shukla and in further view of Araujo (para 7, 24-29).

The Examiner asserts that May teaches a first-point-to-point protocol converted within a network address protocol and that Shukla teaches the packet conversion between protocol layers comprises each protocol layer encapsulating its own header before transmitting to the next layer. In response, Applicants incorporate herein their responses to the Examiner's rejection of claims 1, 12, and 24, and respectfully submit that independent claim 33 is therefore patentable.

G. Section 103 Rejections of Dependent Claims 5 and 15

In the Office Action mailed September 21, 2005, the Examiner states that independent claims are unpatentable under 35 U.S.C. § 103 as obvious over May, Shukla, Araujo and in view of Singhal (para. 39-42).

The Examiner asserts that Singhal teaches the first point-to-point protocol signal further comprises a payload including information that is applied to an application residing at the second client (col. 9, lines 60-62). Applicants' respectfully disagree and submit that Sinhahl teaches information in the network address request header is applied to the application and not the information in the first point-to-point protocol signal. The first point-to-point protocol signal comprising the information is not one of a mere design choice but one of the aspects of the invention wherein the payload of a point-35 U.S.C. § 103 to-point signal is available to network elements that otherwise could not participate in tunneling.

In view of the above, it is respectfully submitted that dependent claims 5 and 15 are patentable.

H. Section 103 Rejections of Dependent Claims 7 and 16

In the Office Action mailed September, 21, 2005, the Examiner states that independent claims are unpatentable under 35 U.S.C. § 103 as obvious over May in view of Shukla in further view of Araujo and in further view of Singhal (para. 39, 44, 45)

The Examiner asserts that Singhal teaches the first point-to-point protocol signal further comprises a payload including at least a portion of an application to be installed on the second client. Applicants' respectfully disagree and submit Singhal teaches adding an AUL table entry used by the core server application. A table entry is a data repository (see e.g., col. 4 lines 24 -

27) wherein an application is executable program. A table entry is completely different than an application.

In view of the above, it is respectfully submitted that dependent claims 7 and 16 are patentable.

I. Conclusion

For the foregoing reasons, Applicants respectfully submit that the rejections set forth in the final Office Action are inapplicable to the pending claims. The honorable Board is therefore respectfully requested to reverse the final rejection of the Examiner and the remand the application to the Examiner with instructions to allow the pending claims. Please grant any extensions of time required to enter this paper. Please charge any appropriate fees due in connection with this paper or credit any overpayments to Deposit Account No. 19-2179.

Respectfully submitted,

Dated: 5/19/06

By: _____

Daniel J. Staudt
Registration No. 34,733
(407) 736-2415

Siemens Corporation
Intellectual Property Department
170 Wood Avenue South
Iselin, New Jersey 08830

Claims Appendix

1. A method of communicating with an element within an enterprise network, comprising:

at a first client, encapsulating a first point-to-point protocol signal within a network address request header, the first point-to-point protocol signal comprising a point-to-point protocol header that includes an identifier of a second client; and

communicating the encapsulated signal toward a tunneling server.

2. (Canceled)

3. The method of claim 1, wherein communicating the encapsulated signal toward a tunneling server comprises communicating the signal toward a router configured to relay network address requests to the tunneling server without referencing a routing table indexed by data channel addresses.

4. The method of claim 3, wherein the identifier comprises a control channel address of the second client, the control channel address being different from any data channel address recognized by the router.

5. The method of claim 1, wherein the first point-to-point protocol signal further comprises a payload including information to be applied to an application residing at the second client.

6. The method of claim 5, wherein the application residing at the second client comprises a maintenance application operable to diagnose operational characteristics of the second client.

7. The method of claim 1, wherein the first point-to-point protocol signal further comprises a payload including at least a portion of an application to be installed on the second client.

8. The method of claim 1, further comprising encapsulating the first point-to-point protocol signal within a tunneling header prior to encapsulating the first point-to-point protocol signal within the network address request header, the tunneling header operable to facilitate a tunneling session between the first client and the tunneling server.

9. The method of claim 8, wherein the tunneling header comprises a tunneling header selected from the group consisting of a Layer Two Tunneling Protocol (L2TP) header, a Point-to-Point Tunneling Protocol (PPTP), or a Layer Two Forwarding (L2F) header.

10. The method of claim 1, further comprising receiving an encapsulated response signal from the tunneling server, the encapsulated response signal comprising a second point-to-point protocol signal responsive to the first point-to-point protocol signal and encapsulated within a network address response header.

11. The method of claim 10, wherein the network address response header comprises a Dynamic Host Configuration Protocol OFFER header or a Bootstrap Protocol RESPONSE header.

12. A computer readable medium operable to execute the following steps on a processor of a computer:

at a first client, encapsulating a first point-to-point protocol signal within a network address request header, the first point-to-point protocol signal comprising a point-to-point protocol header that includes an identifier of a second client; and

communicating the network address request encapsulated signal toward a tunneling server.

13. The computer readable medium of claim 12, wherein communicating the encapsulated signal toward a tunneling server comprises communicating the signal toward a router configured to relay network address requests to the tunneling server without referencing a routing table indexed by data channel addresses.

14. The computer readable medium of claim 13, wherein the identifier comprises a control channel address of the second client, the control channel address being different from any data channel address recognized by the router.

15. The computer readable medium of claim 12, wherein the first point-to-point protocol signal further comprises a payload including information to be applied to an application residing at the second client.

16. The computer readable medium of claim 12, wherein the first point-to-point protocol signal further comprises a payload including at least a portion of an application to be installed on the second client.

17. The computer readable medium of claim 12, further comprising encapsulating the first point-to-point protocol signal within a tunneling header prior to encapsulating the first point-to-point protocol signal within the network address request header, the tunneling header operable to facilitate a tunneling session between the first client and the tunneling server.

18. The computer readable medium of claim 12, further comprising receiving an encapsulated response signal from the tunneling server, the encapsulated response signal comprising a second point-to-point protocol signal responsive to the first point-to-point protocol signal and encapsulated within a network address response header.

19. A method of tunneling in an enterprise network comprising a plurality of clients coupled to a tunneling server by at least one router, the method comprising:

at a first client, generating point-to-point protocol signal;

encapsulating the point-to-point protocol signal within a network address request header;

communicating the encapsulated signal toward a tunneling server operable to identify and remove the network address request header, to encapsulate the point-to-point protocol signal within a network address response header, and to communicate the encapsulated response signal toward a second client.

20. The method of claim 19, communicating the encapsulated signal toward a tunneling server comprises communicating the signal toward a router operable to relay the signal toward the tunneling server without referencing a routing table indexed by data channel addresses.

21. The method of claim 20, wherein the point-to-point protocol signal comprises a control channel address of a second client, the control channel address being different from any data channel address recognized by any router coupled to the tunneling server.

22. The method of claim 19, further comprising encapsulating the point-to-point protocol signal within a tunneling header prior to encapsulating the point-to-point protocol signal within the network address request header, the tunneling header operable to facilitate a tunneling session between the first client and the tunneling server.

23. The method of claim 19, further comprising receiving a response from the second client, the response forwarded from the tunneling server and comprising a point-to-point protocol signal encapsulated within a network address response header.

24. In an enterprise network comprising at least one client coupled to a tunneling server by a router having a routing table indexed by data channel addresses, a first client comprising:

a protocol stack operable to generate a first point-to-point protocol signal comprising a point-to-point protocol header that includes an identifier of a second client; and

a tunneling module operable to encapsulate the first point-to-point encapsulated signal within a network address request header comprising a Dynamic Host Configuration Protocol DISCOVER header or a Bootstrap Protocol REQUEST header;

wherein the first client is operable to communicate the encapsulated signal toward the router for forwarding to the tunneling server without reference to the routing table.

25. (Canceled)

26. The first client of claim 24, wherein the encapsulated signal comprises a tunneling header encapsulating the first point-to-point signal, the tunneling header operable to facilitate a tunneling session between the first client and the tunneling server.

27. The first client of claim 26, wherein the tunneling header comprises a tunneling header selected from the group consisting of a Layer Two Tunneling Protocol (L2TP) header, a Point-to-Point Tunneling Protocol (PPTP), or a Layer Two Forwarding (L2F) header.

28. The first client of claim 24, wherein the second client is coupled to the tunneling server and the first point-to-point protocol signal further comprises information to be applied to an application residing at the second client.

29. The first client of claim 28, wherein the identifier of the second client comprises a control channel address of the second client, the control channel address being distinct from any data channel address used to index a routing table accessible to the router.

30. The first client of claim 28, wherein information comprises information to be applied to a maintenance application residing at the second client and operable to diagnose operational characteristics of the second client.

31. The first client of claim 24, wherein the tunneling module is operable to receive a point-to-point protocol signal encapsulated within a network address response header, the encapsulated response signal having been relayed from the tunneling server through the router without reference to a routing table indexed by data channels.

32. The first client of claim 31, wherein the network address response header comprises a DHCP OFFER header or a Bootstrap Protocol RESPONSE header.

33. (Currently Amended) In an enterprise network, a client having an enterprise protocol stack operable to process signals received from a data channel and associated with a data channel address, the client comprising:

a tunneling module operable to receive a first point-to-point protocol signal encapsulated within a network address response header and to remove the network address response header to expose the first point-to-point protocol signal, the first point-to-point protocol signal comprising

a point-to-point protocol header that includes an identifier of a client, the network address response header; and

a private protocol stack operable to receive the first point-to-point protocol signal from the tunneling module and to communicate at least a portion of a payload of the first point-to-point protocol signal to a socket layer coupled to an application residing at the client.

34. (Canceled)

35. The client of claim 33, wherein the application comprises a maintenance application operable to diagnose operational characteristics of the client.

36. The client of claim 33, wherein the application comprises an application operable to process the at least a portion of the payload and to generate an output to be communicated toward another network element.

37. The client of claim 33, wherein: the private protocol stack is operable to generate a second point-to-point protocol signal comprising a point-to-point protocol header that includes an identifier of a destination network element and a payload carrying at least a portion of the output; and

wherein the tunneling module is operable to encapsulate the second point-to-point signal within a network address request header and communicate the network address request encapsulated signal to a router for relaying toward the destination network element without reference to a routing table indexed by data channel addresses.

38. The client of claim 37, wherein the network address request header comprises a Dynamic Host Configuration Protocol DISCOVER header or a Bootstrap Protocol REQUEST header.

39. The client of claim 33, wherein the first point-to-point protocol signal is encapsulated within a tunneling header and further encapsulated within the network address response header, and wherein the tunneling module is operable to process the tunneling header to maintain a tunneling session between the client and a tunneling server.

40. The client of claim 39, wherein the tunneling header comprises a tunneling header selected from the group consisting of a Layer Two Tunneling Protocol (L2TP) header, a Point-to-Point Tunneling Protocol (PPTP), or a Layer Two Forwarding (L2F) header.

41. The method of Claim 1, wherein the identifier comprises a host name, IP address, or MAC address of the second client, the host name, IP address, or MAC address being different from any host name, IP address, or MAC address recognized by the router.

42. The computer readable medium of Claim 12, wherein the identifier comprises a host name, IP address, or MAC address of the second client, the host name, IP address, or MAC address being different from any host name, IP address, or MAC address recognized by the router.

43. The first client of Claim 24, wherein the identifier comprises a host name, IP address, or MAC address of the second client, the host name, IP address, or MAC address being different from any host name, IP address, or MAC address recognized by the router.

44. The client of Claim 33, wherein the identifier comprises a control channel address of the client, the control channel address being different from any data channel address recognized by the router.

45. The client of Claim 33, wherein the identifier comprises a host name, IP address, or MAC address of the client, the host name, IP address, or MAC address being different from any host name, IP address, or MAC address recognized by the router.

Evidence Appendix

None